UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,885	10/11/2000	Anders Johnson	108339-00010	5015

7590 03/29/2004

SQUIRE SANDERS & DEMPSEY LLP
14th FL
8000 Towers Crescent Drive
Tysons Corner, VA 22182-2700

EXAMINER	
AKPATI, ODAICHE T	
ART UNIT	**PAPER NUMBER**
2135	4

DATE MAILED: 03/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PRG

Office Action Summary	Application No.	Applicant(s)	
	09/685,885	JOHNSON, ANDERS	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 11 October 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6, 11-13, 15, 16, 18-20, 23, 25-30, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al (5577121).

With respect to Claim 1, the limitation of "a random number generating module for generating a random number" is met inherently on column 13, lines 5-10; and "a hash function module in communication with said random number generating module" is inherently met on column 11, lines 60-62; and "a host in communication with said random number generating module" is met inherently on column 13, lines 5-10. This is because the security module which generates the random number is contained within the host (see Fig. 2). Further limitation of "at least one memory in communication with said host" is met on Fig. 2; and "an encryption module in communication with said at least one memory" is met on column 2, lines 1-5, column 13, lines 36-42 and on Fig. 2; and "a comparing device in communication with said encryption module and said hash function module" is met on column 13, lines 36-42 and on column 11, lines 60-63; and "wherein said comparing device compares a first bit string to a second bit string to generate a function enable output for the component" is met on column 13, lines 66-67 and on column 14,

lines 1-7. The confirmation of an established secure session inherently discloses an enable output because a confirmation signal is sent to an external device i.e. the reader/writer. This positive confirmation signal acts as the function enable. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add a function enable to the invention based on the teachings of Davis et al.

With respect to Claim 2, the limitation "wherein said hash function module further comprises a one-way hash function module configured to receive a pre-image input and output a hash value using a one-way hash function algorithm" is met inherently on column 11, lines 60-62 and on column 14, lines 43-47.

With respect to Claim 3, the limitation of "wherein said encryption module further comprises a public key encryption module, said public key encryption module being configured to receive a public key and a guess passcode from said at least one memory as inputs and generate a ciphertext bit string as an output" is met on column 10, lines 53-55 and on column 13, lines 55-63.

With respect to Claim 4, the limitation of "a guess register in communication with said host and said encryption module, said guess register being configured to receive a guess passcode from said host" is met on column 13, lines 63-65 and on Fig. 2; and "a public key module in communication with said encryption module, said public key module being configured to store a public key therein" is met inherently on column 10, lines 53-55.

With respect to Claim 6, the limitation of "a selecting device for selecting at least one of the function enable output and a bonding option output" is met on column 2, lines 5-9.

With respect to Claim 11, the limitation of "a ciphertext bit string generated by the encryption module" is met on column 13, lines 36-42.

With respect to Claim 12, the limitation of "said second bit string further comprises a hash value generated by said hash function module" is met on column 11, lines 60-62.

With respect to Claim 13, 23 the limitation of "wherein said comparing device further comprises a comparator" is met inherently on column 2, lines 6-9.

With respect to Claim 15, the limitation of "means for generating a random bit string" is met on column 13, lines 5-10; and "a hash function module in communication with said means for generating" is met on column 11, lines 60-62; and "means for acquiring a guess passcode in communication with said means for generating" is met on column 14, lines 1-3; and "an encryption module in communication with said means for acquiring" is met on column 14, lines 3-7; and "a comparing device in communication with said encryption module and said hash function module, said comparing device having an output for transmitting a functionality enable signal therefrom" is met on column 14, lines 3-7.

With respect to Claim 16, the limitation of "wherein said means for generating further comprises a random number generating module, wherein said module is configured to receive an initiate signal and output a random number" is met on column 13, lines 5-10.

With respect to Claim 18, the limitation of "wherein said hash function module further comprises a one-way hash function module configured to receive a pre-image input and output a hash value in accordance with a one-way hash function algorithm" is met on column 11, lines 60-62.

With respect to claim 19, the limitation of "a host in communication with said means for generating" is met on column 11, lines 19-24. The POS terminal represents the host. Further limitation of "a guess register in communication with said host" is met on Fig. 2. The memory of the SVC represents the guess register. The limitation of "wherein said host is configured to receive a guess passcode from a manufacturer corresponding to the random bit string" is met on column 11, lines 6-15.

With respect to Claim 20, the limitation of "a public key encryption module" is met on column 10, lines 53-55; and "a public key module in communication with said public key encryption module" is met on column 13, lines 36-42 and "wherein said public key encryption module is configured to receive a public key from said public key module and a guess passcode from said means for acquiring, and generate a ciphertext bit string therefrom" is met on column 13, lines 55-63.

With respect to Claim 25, the limitation of "generating a random number" is met on column 13, lines 6-8; and "calculating a first bit string from the random number" is met on column 13, lines 9-10 and 18-25; and "determining a second bit string corresponding to the random number" is met on column 13, lines 36-46; and "encrypting the second bit string with a public key to generate a third bit string" is met on column 13, lines 36-42; and "comparing the third bit string to the first bit string to determine a match; outputting a function enable signal in accordance with the comparison" is met on column 13, lines 53-55. The confirmation signal represents the enable signal.

With respect to Claim 26, the limitation of "wherein said step of calculating a first bit string further comprises calculating a hash value of said random number" is met on column 17, lines 45-52 and column 14, lines 43-47.

With respect to Claim 27, the limitation of "transmitting the random number to a manufacturer" is met on column 13, lines 8-10; and "calculating a guess passcode corresponding to the random number" is met on column 13, lines 18-22; and "receiving the guess passcode in a host" is met on column 13, lines 23-29.

With respect to Claim 28, the limitation of "receiving a guess passcode from a host" is met on column 13, lines 55-60; and "receiving a public key and encrypting the guess passcode and the public key to generate a ciphertext bit string" is met on column 13, lines 55-63.

With respect to Claim 29, the limitation of "receiving the third bit string at a first input of a comparator; and receiving the first bit string at a second input of the comparator; determining if the first bit string matched the second bit string" is met on column 13, lines 66-67 and on column 14, lines 1-3; and "outputting a match signal if a match is determined" is met on column 14, lines 3-7.

With respect to Claim 30, the limitation of "wherein said outputting step further comprises the step of determining a final output enable signal from a bonding option output signal and the function enable signal" is met inherently on column 14, lines 3-10.

With respect to Claim 32, the limitation of "wherein said transmitting step further comprises communicating with the manufacturer through at least one of an internet connection, a dial up connection, and a voice connection to obtain the guess passcode" is met on column 17, lines 18-22.

Claims 5, 7-10, 17, 21, 22, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al (5577121) in view of Wang (5500808).

With respect to Claims 5, 7-10, 17, 21, 22 and 31 all the limitation is expressly met by Davis et al except the limitation disclosed by the claims listed. However the limitations of the claims listed are silently revealed in Davis et al with respect to the teachings of Wang on column 1, lines 55-59.

It would have been obvious at the time the invention was made to combine the teachings of Wang within the system of Davis et al because it is a well known method to convert a series of inventive steps into equivalent logic gates that perform the same functions as the inventive steps, but in hardware (see Wang, column 1, lines 55-59). It is obvious because this is a well known method in the art of implementing inventive steps into a working hardware construct by conversion to logic gates that implement the inventive steps. It would be impossible to implement the inventive steps in hardware if it weren't converted as disclosed in the invention.

Claims 14, 24 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al (5577121) in view of Conley et al (6651107 B1).

With respect to Claim 14, 24 and 33, all the limitation is met by Davis et al except the limitation disclosed below.

The limitation of "component further comprises at least one of a network switch and a media access controller" is met by Conley et al in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Conley et al within the system of Davis et al because a network switch and a media access controller are necessary for a node to gain access to the internet and vice versa.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA